**IT Applications, Ch 7, Information Management**

Threats to the integrity and security of data and information stored, communicated and disposed of by organisations.

Complete the following from p 270-

**Deliberate threats**

1. When does intentional damage occur?

Intentional damage occurs when the computer suffers a virus, hacking or tampering with files.

1. Unauthorised access is both physical and logical. Explain what this means?

Physical unauthorised access involves stealing or breaking equipment, whereas gaining access to restricted files on the internet is a logical breach.

1. Computer Virus
   1. Describe the nature of this virus.

A computer virus is an infection that affects the operation system of the computer, carrying commands that can seek and destroy or transfer restricted files.

* 1. What is the main purpose of a virus?

The computer virus is designed to affect the running of the PC in a manner unintended by its user.

* 1. What is meant by the term, payload?

The payload of the virus is the action that it is designed to carry out.

* 1. Describe a worm?

A worm is a virus that attaches to an email, and spreads to other emails that sit in the same server. Its main purpose is to slow down and crash email servers due to an overload in electronic traffic.

* 1. List the other types of viruses, p 272, fig. 7-10.

Other types of viruses include boot infectors, executables, macros, time bombs, logic bombs, worms, Trajan horses, residents and polymorphics.

* 1. How do viruses mainly spread?

Viruses mainly spread through an email attachment or the transfer of infected files on removable storage devices.

1. Hacking/Cracking
   1. Who is a hacker and what damage do they cause?

A hacker is someone who breaks into an information system and looks for interesting or confidential material they may contain. They may then exploit these details, revealing confidential information to other criminals.

1. Tampering with files
   1. Describe how employees tamper with files.

Employees may tamper with files by accessing confidential information without authorisation and changing or deleting records.

* 1. What is industrial sabotage?

Industrial sabotage involves countries that are attractive to investors, but have little money of their own. Corrupt government agencies can then demand large amounts of money to allow companies to run their businesses.

1. Information theft
   1. Why does this occur?

Information theft occurs because a company wants to find an edge over its competitors.

1. Vandalism of hardware

Vandalism of hardware can occur because the vandals want to cause havoc to others. For example, destroying a train ticket machine to prevent users from getting their tickets, or jamming phone signals, etc.

1. Theft of hardware

Theft occurs when there is a large demand for a product. Often, smaller objects that are easier to smuggle and bring greater return are stolen, such as RAM chips, hard disks, digital cameras, etc. Any important data stored on these can also be stolen.

**Accidental threats**

1. User error
   1. List some common examples of user error.

Examples include not knowing how to operate the software properly, overwriting information or formatting disks.

* 1. What processes are in place to limit user error.

To limit user error, most software programs have an auto save function which regularly backs up the information if it were to be closed without saving, crashed etc. Pop-up windows asking you to save before closing, and requests for confirmation also limit these errors.

1. Failure to follow file-management procedures
   1. List common errors of employees in saving files.

Common errors in employees saving files include leaving off file extensions, using non descriptive names for saving, and improperly using folders.

**Technical Failure**

1. List some examples of technical failure.

Technical failures that may occur include hardware failures, or physical damage due to fire, water, or electricity surges, and general breakage.

**Consequences of violating security and privacy measures, p 278**

1. List three important consequences if security measures are violated.

The consequences of security violation include breaches in privacy, loss of intellectual property and loss of income due to unavailability of information or services.